CLAIMS

What is claimed is:

1. A method comprising:

obtaining an integrity hash of rights information stored at a client device, said rights information being associated with content stored at the client device;

encrypting the integrity hash using a client device key to generate an encrypted hash, said client device key being externally inaccessible from the client device; and

storing the encrypted hash on the client device.

2. The method of claim 1 wherein obtaining the integrity hash comprises:

receiving the integrity hash from a server device.

3. The method of claim 1 wherein obtaining the integrity hash comprises:

generating the integrity hash on the client device.

4. The method of claim 3 wherein generating the integrity hash on the client device comprises:

applying the client device key in a combination with the rights information; and

determining the integrity hash from the combination of the rights information and the client device key.

5. The method of claim 1 wherein the integrity hash comprises a first integrity hash, the method further comprising:

obtaining a second integrity hash of the rights information; and

storing the second integrity hash on the client device in a clear form.

6. The method of claim 5 wherein obtaining the second integrity hash comprises:

receiving the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key.

7. The method of claim 5 wherein obtaining the first integrity hash comprises:

applying the client device key in a combination with the rights information and the second integrity hash; and

determining the first integrity hash from the combination of the rights information, the second integrity hash, and the client device key.

8. The method of claim 1 further comprising:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

9. The method of claim 1 further comprising:

generating a validation hash from at least the rights information;

decrypting the encrypted hash to recover the integrity hash; and

comparing the validation hash to the integrity hash to detect tampering with the rights information.

10. The method of claim 9 further comprising:

disabling the content on the client device if tampering is detected.

11. The method of claim 1 further comprising:

storing the rights information on the client device in a clear form.

12. The method of claim 10 further comprising:

reading the rights information from the client device in the clear form out to a server device.

13. The method of claim 1 wherein the rights information comprise usage information, the method further comprising:

tracking usage of the content;

updating the rights information with changes in usage;

regenerating, re-encrypting, and restoring the integrity hash on the client device for each update of the rights information.

14. The method of claim 1 wherein the integrity hash comprises a Hash Message Authentication Code (HMAC).

15. The method of claim 1 wherein the client device key comprises a code embedded in hardware of the client device having no externally accessible data path.

16. The method of claim 1 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

17. The method of claim 1 further comprising at least one of:

downloading the rights information from a server device; and

installing a storage medium having the rights information stored thereon.

18. The method of claim 1 wherein the rights information grant unlimited play for the content on the client device.

19. The method of claim 3 wherein generating the integrity hash comprises generating the integrity hash in trusted hardware.

20. A method comprising:

obtaining a first integrity hash of rights information stored at a client device, said rights information being associated with content stored at the client device, said

first integrity hash having been generated using an external key as an integrity secret;

obtaining a second integrity hash of the rights information;

encrypting the second integrity hash using a client device key to generate an encrypted hash, said client device key being externally inaccessible from the client device;

storing the rights information and the first integrity hash at the client device in a clear form; and

storing the encrypted hash at the client device.

21. The method of claim 20 further comprising:

receiving a content key at the client device for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

22. The method of claim 20 wherein obtaining the first integrity hash comprises:

receiving the external key at the client device; and

generating the first integrity hash at the client device using the external key.

23. The method of claim 20 wherein obtaining the first integrity hash comprises:

receiving the first integrity hash from a server device.

24. The method of claim 20 wherein obtaining the second integrity hash comprises:

receiving the second integrity hash from a server device; and

receiving a key used by the server device to generate the second integrity hash.

25. The method of claim 20 wherein obtaining the second integrity hash comprises:

generating the second integrity hash at the client device using the client device key as an integrity secret.

26. The method of claim 20 further comprising:

reading the rights information and the first integrity hash from the client device in the clear form out to a server device;

generating a validation hash, using the external key, of at least the rights information read from the client device; and

comparing the validation hash to the first integrity hash to detect tampering.

27. The method of claim 20 further comprising:

generating a validation hash from at least the rights information;

decrypting the encrypted hash using the client device key to recover the second integrity hash; and

comparing the validation hash to the second integrity hash to detect tampering.

28. The method of claim 20 wherein the rights information comprise usage information, the method further comprising:

tracking usage of the content; and

updating the rights information with changes in usage.

29. The method of claim 28 further comprising:

regenerating and restoring the first integrity hash on the client device for each update.

30. The method of claim 28 further comprising:

regenerating, re-encrypting, and restoring the second integrity hash on the client device for each update.

31. A method comprising:

generating a validation hash from at least rights information associated with content stored on a client device;

decrypting an encrypted hash to recover an integrity hash using a client device key that is externally inaccessible from the client device, said integrity hash having been previously generated from at least the rights information associated with the content; and

comparing the validation hash to the integrity hash to detect tampering with the rights information.

32. The method of claim 31 further comprising:

disabling the content on the client device if tampering is detected.

33. The method of claim 31 further comprising:

receiving a usage request for the content stored at the client device, said usage request to initiate generation of the validation hash and comparison to the integrity hash; and

permitting usage only if the content is not disabled.

34. A client device comprising:

a register to store a client device key, said register being externally inaccessible from the client device;

a memory to store content and rights information associated with the content, said memory being externally accessible;

hash circuitry to obtain an integrity hash of the rights information; and

encryption circuitry to encrypt the integrity hash using the client device key to generate an encrypted hash;

said memory to store the encrypted hash.

35. The client device of claim 34 wherein the hash circuitry is to obtain the integrity hash from a server device.

36. The client device of claim 34 wherein the hash circuitry is to generate the integrity hash on the client device.

37. The client device of claim 36 wherein, to generate the integrity hash, the hash circuitry is to apply the client device key in a combination with the rights information, and to determine the integrity hash from the combination of the rights information and the client device key.

38. The client device of claim 34 wherein the integrity hash comprises a first integrity hash, the hash circuitry further to obtain a second integrity hash of the rights information, said memory to store the second integrity hash in a clear form.

39. The client device of claim 38 wherein, to obtain the second integrity hash, the hash circuitry is to receive the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key.

40. The client device of claim 38 wherein, to obtain the first integrity hash, the hash circuitry is to apply the client device key in a combination with the rights information and the second integrity hash, and to determine the first integrity hash from the combination of the rights information, the second integrity hash, and the client device key.

41. The client device of claim 34 wherein

the encryption circuitry is to encrypt a content key for the content using the client device key to generate an encrypted content key; and

the memory is to store the encrypted content key on the client device.

42. The client device of claim 34 wherein

the hash circuitry is to generate a validation hash from at least the rights information; and

the encryption circuitry is to decrypt the encrypted hash to recover the integrity hash;

the client device further comprising:

a comparator to compare the validation hash to the integrity hash to detect tampering with the rights information.

43. The client device of claim 42 further comprising:

a content controller to disable the content on the client device if tampering is detected.

44. The client device of claim 34 wherein the memory is to store the rights information in a clear form.

45. The client device of claim 34 wherein the rights information comprise usage information, the client device further comprising:

tracking circuitry to track usage of the content and update the rights information changes in usage;

wherein the hash circuitry and the encryption circuitry are to regenerate, re-encrypt, and restore the integrity hash in the memory for each update of the rights information.

46. The client device of claim 34 wherein the client device comprises at least one of an MP3 player, a personal data assistant, and cellular phone.

47. The client device of claim 34 further comprising at least one of:

an input port to download the rights information from a server device; and

a storage medium port to receive a storage medium having the rights information stored thereon.

48. The client device of claim 47 wherein the memory at least partially comprises the storage medium.

49. A machine readable medium having stored thereon machine executable instructions, the execution of which to implement a method comprising:

receiving rights information at a client device, said rights information being associated with content stored on the client device, said client device having a client device key that is externally inaccessible from the client device;

obtaining an integrity hash of the rights information;

encrypting the integrity hash using the client device key to generate an encrypted hash; and

storing the encrypted hash on the client device.

50. The machine readable medium of claim 49 wherein obtaining the integrity hash comprises:

receiving the integrity hash from a server device.

51. The machine readable medium of claim 49 wherein obtaining the integrity hash comprises:

generating the integrity hash on the client device.

52. The machine readable medium of claim 49 wherein generating the integrity hash on the client device comprises:

applying the client device key in a combination with the rights information; and

determining the integrity hash from the combination of the rights information and the client device key.

53. The machine readable medium of claim 49 wherein the integrity hash comprises a first integrity hash, the method further comprising:

obtaining a second integrity hash of the rights information; and

storing the second integrity hash on the client device in a clear form.

54. The machine readable medium of claim 53 wherein obtaining the second integrity hash comprises:

receiving the second integrity hash from a server device, said server device having generated the second integrity hash using a server device key.

55. The machine readable medium of claim 53 wherein obtaining the first integrity hash comprises:

applying the client device key in a combination with the rights information and the second integrity hash; and

determining the first integrity hash from the combination of the rights information, the second integrity hash, and the client device key.

56. The machine readable medium of claim 49 wherein the method further comprises:

receiving, at the client device, a content key for the content;

encrypting the content key using the client device key to generate an encrypted content key; and

storing the encrypted content key on the client device.

57. The machine readable medium of claim 49 wherein the method further comprises:

generating a validation hash from at least the rights information;

decrypting the encrypted hash to recover the integrity hash; and

comparing the validation hash to the integrity hash to detect tampering with the rights information.

58. The machine readable medium of claim 57 wherein the method further comprises:

disabling the content on the client device if tampering is detected.

59. The machine readable medium of claim 49 wherein the method further comprises:

storing the rights information on the client device in a clear form.

60. The machine readable medium of claim 59 wherein the method further comprises:

reading the rights information from the client device in the clear form out to a server device.

61. The machine readable medium of claim 49 wherein the rights information comprise usage information, the method further comprising:

tracking usage of the content;

updating the rights information with changes in usage;

regenerating, re-encrypting, and restoring the integrity hash on the client device for each update of the rights information.